

## INFORMATION SECURITY AWARENESS TRAINING – FISCAL YEAR 2016

### PAPER-BASED EXAM 3

1. The goal of ISS is to:

- a. Encourage hackers.
- b. Protect information systems against unauthorized access
- c. Decrease availability of systems
- d. Both encourage hackers and decrease availability of systems

2. The Federal Information Security Management Act (FISMA):

- a. Defines national security systems
- b. All of the answers are correct
- c. Requires a greater level of protection for Government information systems that contain Privacy Act information
- d. Mandates a computer security program at all federal agencies

3. What is not PII?

- a. Employment History
- b. Information about or associated with an individual
- c. Place of birth
- d. Zip Code

4. Which of the following is an example of a security incident?
- a. Attempts to send electronic junk mail in the form of commercial announcements
  - b. All of these are security incidents
  - c. Loss of a government laptop containing personnel information
  - d. Attempts by unidentified or unauthorized people to obtain sensitive personal or business information
5. Lauren gets an e-mail with an attachment from the director of her agency. It has a file attachment with an unfamiliar file extension. Lauren should do all of the following except:
- a. Call the help-desk for advice on handling the situation
  - b. Verify that the sender sent the e-mail and attachment
  - c. Be suspicious of this e-mail and attachment
  - d. Open the attachment
6. Thomas visits a web site that unbeknownst to him has transmitted malicious code to his computer. This malicious code can do all of the following to his computer except:
- a. Corrupt files
  - b. Cause his computer to catch fire
  - c. Erase his hard drive
  - d. Enable others to gain access to his computer

7. Diana has her paycheck deposited directly from her employer's account into her checking account. This is an example of what?

- a. Phishing
- b. E-commerce
- c. Cookies
- d. Telework

8. Nancy just read in her local newspaper that the FBI has determined that this crime is growing more rapidly than many others -- Which is it?

- a. Embezzlement
- b. Identity theft
- c. Fraud
- d. Murder

9. Cookies contain information about you. This information, if not encrypted, could be viewed by a third party. The best practice to prevent this from happening is:

- a. Ensure your browser is set to not accept cookies
- b. Visit only web sites that use ActiveX or JavaScript code
- c. Do not visit non-government web sites
- d. Install spyware software

10. Jacob collects movies. He found a way to get movies at no cost using a service where he shares his computer's content with other users. He sets up his work computer to use this service. This is an example of the following vulnerability:

- a. Mobile code
- b. Peer-to-peer technology
- c. Social engineering
- d. Software flaw

11. For Official Use Only (FOUO) and Controlled Unclassified Information (CUI) may include all of the following except:

- a. Payroll information
- b. Personnel information
- c. Secret information
- d. Sensitive information

12. All of the following are acceptable procedures for backing up classified information except:

- a. Back classified information up daily
- b. Store backups in your desk drawer
- c. Label backups with sensitivity labels
- d. Store backups at an approved secure location